Charterhouse Group Acceptable Use Policy

1. Introduction

1.1. This Acceptable Use Policy ("**AUP**") applies to Users accessing and using Equipment, Software and/or Services provided by Charterhouse Voice & Data Limited (**"Supplier"**). "Pentesec" and "Symity" are trading names of Charterhouse Voice & Data Limited. Defined terms used in this AUP shall have the meaning set out in the Charterhouse General Terms & Conditions at cvdgroup.com/legal (**"Terms & Conditions"**).

1.2. Supplier may change the AUP from time-to-time and publish the latest version on the Supplier website at cvdgroup.com/legal, with the latest version being effective immediately on publication.

1.3. "**Users**" means the Customer and the Customer's employees, agents, contractors, end-customers and other personnel, end-users, or anyone else who uses or accesses the Services.

1.4. It is the Customer's responsibility to procure Users adherence to this AUP, and the Customer remains liable for any breaches of this AUP by Users.

1.5. The Customer is responsible for keeping its contact details with Supplier up to date. Where Supplier is unable to contact the Customer at an address you have given, it will address any email correspondence to 'postmaster' at your domain address/es.

2. Use of the Services

2.1. In addition to the Customer's obligations under the Terms & Conditions, in using the Equipment, Software and/or Services, the Customer agrees to (and shall procure that all Users agree to):

(a) abide by all local, national, and international laws and regulations applicable to Customer's use of the Equipment, Software and/or Services, including without limitation all laws and administrative regulations relating to the control of exports of commodities and technical and/or Personal Data, and shall not allow any of its personnel or Data Subjects to access or use the Equipment, Software and/or Services in violation of any export embargo, prohibition or restriction;

(b) provide any required notifications to Data Subjects, and obtain all rights and requisite consents from Data Subjects in accordance with all applicable Data Protection Laws and other laws in relation to the collection, use, disclosure, creation and processing of Personal Data in connection with the Agreement and the use and delivery of the Equipment, Software and/or Services;

(c) not use the Equipment, Software and/or Services for illegal purposes;

(d) not knowingly upload or distribute in any way files that contain viruses, corrupted files, or any other similar software or programs that may damage the operation of the hosted environment, the Services, or another's computer;

(e) not knowingly interfere with another customer's use and enjoyment of equipment, software and/or services or another entity's use and enjoyment of similar services;

(f) not knowingly engage in contests, chain letters or post or transmit "junk mail," "spam," "chain letters," or unsolicited mass distribution of email or other messages through or in any way using the Equipment, Software and/or Services;

(g) not to interfere or disrupt the Services, any networks through which the Services are delivered or on which they rely, or any other infrastructure related to the Services;

(h) not to post, promote or transmit through the Equipment, Software and/or Services any unlawful, harassing, defamatory, privacy invasive, abusive, threatening, offensive, harmful, vulgar, obscene, tortuous, hateful, racially, ethnically or otherwise objectionable information or content of any kind or nature;

(i) not to transmit or post any material that encourages conduct that could constitute a criminal offense or give rise to civil liability. Supplier may remove any violating content posted on the Services or transmitted through the Services, without notice to Customer;

(j) not to inspect, possess, use, copy, modify, reverse engineer, or create derivative works of or attempt to discover the source code used to create any program or other component of the Equipment, Software and/or Services, except as expressly permitted by applicable laws;

(k) not to probe, scan or test the efficacy or vulnerability of the Software and/or Services, or take any action in an effort to circumvent or undermine the Software and/or Services, except for the legitimate testing of the Software and/or Services in coordination with Supplier in connection with considering an order of Software and/Services as part of any proof of concept or trial;

(l) not to send, receive or store any material which infringes copyright, trademark or other any other intellectual property law, or to upload, post, publish or transmit any information or software that is protected by copyright or other ownership rights without the permission of its owner;

(m) not to sell, resell, license, sublicense, distribute, offer, rent or lease the Software and/or Services, or otherwise make the Software and/or Services or any part thereof (including associated documentation) available to any third party, or use the Software and/or Services as an agent or on behalf of any party other than Customer and any permitted affiliates; and

(n) not to trunk or forward extensions or numbers associated with the Software and/or Services to a private branch exchange or key system or to other numbers that can process multiple calls simultaneously.

3. Data, System Security and Backup

3.1. In addition to the Customer's obligations under the Terms & Conditions, the Customer accepts that:

(a) except where data back-up is expressly included in the Services (and only to the extent described therein), Users are responsible for the backup of their data;

(b) Users are responsible for the security of their own devices that are directly or indirectly connected to the Services;

(c) Login details may not be shared and passwords must be regularly changed, meet minimum complexity criteria and kept secure;

(d) It may not to perform any form of security testing (also known as penetration testing) on any system Supplier manages without Supplier's express prior written authorisation; and

(e) The security of the services used by you is your responsibility. It is also your responsibility to ensure that you keep your passwords secure. We are not responsible for any negative consequences (e.g. lost or corrupted files) incurred by your failure to employ adequate security measures.

4. Fair Usage

4.1. The Customer acknowledges that certain Services may have fair usage policies and where these are applicable, the Customer shall comply with these fair usage policies.

5. Enforcement

5.1. Complaints regarding the conduct of a User on our network will be accepted by sending an email to service.desk@cvdgroup.com and via all other standard abuse reporting mechanisms. We must be able to verify each instance of abuse, and so each complaint must include the full headers and/or complete body of the offending message (where appropriate) or other forms of quantitative, supportive evidence. Submitting all relevant evidence in the original abuse report will significantly speed up the resolution of the issue by Supplier.

5.2. We reserve the right to investigate any suspected violation(s) of this AUP. When we become aware of possible violations, we may initiate an investigation, which may include gathering information from the User involved and the complaining party, if any, and examination of material on our servers, networks or any other equipment associated with the Services.

5.3. A breach of this AUP by Customer is a material breach of the Agreement.

5.4. Without prejudice to Supplier's other rights and remedies under the Terms & Conditions, Supplier may, in Supplier's sole discretion, warn, suspend, restrict or terminate a User's service for violation of any of part of this AUP at any time and without warning.